Bitcoin, "una innovadora red de pagos y una nueva clase de dinero"

Inés Fandos Duce

En 2014 el 37% de los españoles afirmó haber solicitado o comprado bienes o servicios a través de Internet, cifra que asciende al 50% en el conjunto de la Unión Europea[1]. Estas cifras reflejan apenas una pequeña parte de la digitalización de nuestra sociedad y nuestra economía.

En un mundo tan global la idea de un sistema de pago descentralizado resulta muy interesante. En 1982 David Chaum proponía un sistema criptográfico de pagos no rastreables en "*Blind Signatures for untraceable payments*", y en 1990 fundaba DigiCash. En 1998 Wei Dai describía una moneda criptográfica a la que denominaba *b-money*. Diez años más tarde, en diciembre de 2008, Satoshi Nakamoto publicaba "*Bitcoin: A Peer-to-Peer Electronic Cash System*", documento que recogía la necesidad de un nuevo modelo de pago electrónico sin intermediarios y desarrollaba la especificación del protocolo. En enero de 2009 se lanza la primera versión de Bitcoin.

Bitcoin se describe como "una innovadora red de pagos y una nueva clase de dinero"[2]. De esta forma, se trata por un lado de una red peer-to-peer que permite a sus usuarios realizar transacciones sin la intervención de una autoridad central, y por otro, de la propia moneda electrónica en la que se realizan dichas transacciones.

El funcionamiento de Bitcoin se basa en una contabilidad pública o *block chain,* que recoge todas las transacciones procesadas por la red, verificadas por el conjunto de nodos de Bitcoin. La autenticidad de las transacciones se garantiza a través de firmas digitales asociadas a las direcciones de envío. Cualquiera puede participar en el proceso de verificación de transacciones, que además se recompensa en *bitcoins.* Este proceso se conoce como *mining* o minería.

Todo el software necesario para el uso del protocolo se trata de software libre, gestionado por la comunidad de usuarios. Esta característica, junto con el modelo de descentralización, dota de gran transparencia al sistema.

El sistema Bitcoin tiene múltiples ventajas e inconvenientes asociados. En primer lugar, ofrece una gran libertad de pagos, al ser el envío y la recepción de dinero casi instantáneos. Además, las tasas asociadas son muy reducidas o incluso inexistentes, y las transacciones son seguras e irreversibles. La existencia de comisiones voluntarias a cambio de rapidez en la verificación permite remunerar a los mineros, indispensables para el funcionamiento del sistema. Otra de las funciones de las tasas es la protección frente a ataques de denegación de servicio.

Asimismo, cabe destacar que las transacciones no contienen datos personales o privados de los clientes, por lo que el sistema garantiza en alto grado el anonimato, siempre y cuando se use en conjunto con los múltiples mecanismos que se han desarrollado con la intención de proteger la privacidad de los usuarios.

Los *bitcoins* cumplen indiscutiblemente con la mayoría de las características que ha de tener una mercancía para poder adoptarse como dinero. Es escaso, ya que tiende a un límite máximo de *bitcoins* en circulación de 21 millones. Es altamente portable y divisible, ya que cada *bitcoin* puede dividirse hasta ocho cifras decimales, y se podría dividir en unidades aún más pequeñas en caso necesario. Es duradero, puesto que no se degrada con el tiempo, como podría hacerlo un producto perecedero; y por último es imposible de falsificar.

La última característica, la homogeneidad, puede ser objeto de discusión. Esta propiedad refleja el hecho de que dos monedas del mismo valor han de ser indistinguibles, y no deben existir razones para preferir una sobre otra. Se podría considerar que los *bitcoins* no cumplen esta última propiedad, puesto que recogen en ellos todas las transacciones en las que han participado. Una persona podría querer evitar un *bitcoin* que haya estado relacionado con determinadas actividades.

Se han desarrollado múltiples iniciativas con el objetivo de "validar *bitcoins*", un proceso que precisamente atacaría la homogeneidad de las mismas. Este es el caso de *Coin Validation*, surgida en 2013 generando gran polémica a su alrededor[3, 4]. Su objetivo era crear un sistema de seguimiento de la propiedad de los *bitcoin*, con el fin de evitar actores malintencionados, y de dotar de cierta regulación a Bitcoin. Sin embargo, esto permitiría la existencia de listas negras, que acabarían con la homogeneidad de la moneda[5].

La propia web de Bitcoin avisa sobre las desventajas de su sistema, aunque desaparecerían con la expansión de su uso, siendo uno de sus principales problemas la volatilidad. Desde su aparición en enero de 2009, el valor de los *bitcoins* en comparación con otras divisas de curso legal presenta continuas fluctuaciones. Sin embargo, la mayoría de comerciantes que los aceptan utilizan servicios de pago como BitPay y Coinbase, que permiten mostrar los precios en monedas convencionales como el dólar o el euro, convirtiéndolos a *bitcoins* en el momento de la compra, y volviéndolos a convertir a la moneda local del comerciante una vez finalizada la transacción. Este mecanismo permite así evitar a corto plazo las fluctuaciones en el valor del *bitcoin*.

Otro de los inconvenientes de *bitcoin*, que afecta en gran parte a la volatilidad, es el grado de aceptación. La capitalización de mercado es actualmente de 4800 millones de dólares[6]. Esta cantidad representa menos del 5% de la capitalización bursátil de Inditex[7], y alrededor del 0,35% del PIB de España en 2014[8]. Se trata por tanto de una cifra muy pequeña. Es por ello que, teniendo en cuenta este valor, y dado que el

volumen de transacciones que se realizan a través de Bitcoin aún es relativamente bajo, cualquier intercambio afecta significativamente al precio.

Figura 1 – Evolución del precio del *bitcoin* en dólares[9]. Fuente: blockchain.info

Se puede encontrar un ejemplo en el caso de Silk Road, un mercado negro online lanzado en 2011, cuyas compras se realizaban en su mayoría en *bitcoins*. En el momento de su cierre, en octubre de 2013, se incautaron unos 174 000 *bitcoins*, aproximadamente el 1,5% del total en circulación en aquel momento. Una venta masiva hubiera causado una caída considerable en su cotización.

El caso de Silk Road representa además la gran preocupación acerca del papel que puede representar Bitcoin en actividades ilegales. Esta preocupación se agrava en parte por la ausencia de un regulador. El carácter descentralizado de Bitcoin provoca la falta de respaldo en caso de que su valor descienda bruscamente. Esta es precisamente una de las funciones de los Bancos Centrales: asegurar en la medida de lo posible la estabilidad monetaria.

En resumen, el sistema Bitcoin ofrece grandes avances al proporcionar un sistema de transferencia de valor revolucionario sin intermediarios, sin necesidad de intercambiar datos personales más allá de los seudónimos que representan las claves públicas. Durante el proceso de desarrollo surgen múltiples riesgos asociados, como la volatilidad de su valor, que puede fomentar la especulación o incluso frenar dicho desarrollo. Además, la ausencia de un regulador hace que no existan garantías en caso de que su valor se desplome rápidamente. Al margen de ello, se trata de un modelo que en un futuro, solventados los obstáculos mencionados, puede llegar a tener un gran éxito, puesto que facilita enormemente las transacciones entre clientes situados

en cualquier parte del mundo, evitando las tasas que imponen los sistemas actuales como VISA, PayPal o las transferencias bancarias tradicionales.

---

[1] Eurostat; *Internet purchases by individuals*; http://ec.europa.eu/eurostat; Último acceso 14 de noviembre de 2015.
[2] https://bitcoin.org/es/; Último acceso 14 de noviembre de 2015.
[3] Bradbury, Danny; *Anti-Theft Bitcoin Tracking Proposals Divide Bitcoin Community*; CoinDesk; http://www.coindesk.com/bitcoin-tracking-proposal-divides-bitcoin-community/; Último acceso 14 de noviembre de 2015.
[4] Buterin, Vitalik; *Why The Bitcoin Greenlist is Structurally Dangerous to the Bitcoin Ecosystem*; Bitcoin Magazine; https://bitcoinmagazine.com/articles/why-the-bitcoin-greenlist-is-structurally-dangerous-to-the-bitcoin-ecosystem-1384492133; Último acceso 14 de noviembre de 2015.
[5] Hill, Kashmir; *Sanitizing Bitcoin: This Company Wants To Track 'Clean' Bitcoin Accounts*; http://www.forbes.com/sites/kashmirhill/2013/11/13/sanitizing-bitcoin-coin-validation/;Último acceso 14 de noviembre de 2015.
[6] https://bitcoincharts.com/bitcoin/ Último acceso 14 de noviembre de 2015.
[7] http://www.eleconomista.es/indice/IBEX-35 Último acceso 14 de noviembre de 2015.
[8] http://data.worldbank.org/indicator/NY.GDP.MKTP.CD Último acceso 14 de noviembre de 2015.
[9] https://blockchain.info/es/charts Último acceso 14 de noviembre de 2015.